AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type, and wherein each dynamic behavior evaluation module records ~~some execution behaviors~~interesting function calls that ~~of~~ the code module makes as it is executed, wherein the interesting function calls are specified by a user and comprise a subset of all function calls that the code module makes, wherein only the interesting function calls, but not all function calls, that the code module makes during execution in the dynamic behavior evaluation module~~a plurality of different execution behaviors of the code module~~ are recorded into a behavior signature corresponding to the code module;

a management module, wherein the management module obtains the code module, and wherein the management module evaluates the code module to determine the code module's type, and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the code module's type;

a malware behavior signature store storing at least one known malware behavior signature of a known malware, wherein each of the at least one known malware behavior signature is comprised of only interesting function calls as specified by the user;

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the interesting function calls recorded in the behavior signature of the code module match the interesting function calls in any of the known malware behavior signatures; and ~~plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware; and~~

wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the ~~plurality of different execution~~

~~behaviors~~interesting function calls recorded in the behavior signature of the code module match ~~at least one of a plurality of different subsets of execution behaviors recorded~~the interesting function calls in a behavior signature of the known malware~~, wherein the different subsets of execution behaviors are pre-specified for the known malware~~.

2. (Currently Amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one behavior evaluation means, wherein each behavior evaluation means provides a virtual environment for executing a code module of a particular type, and wherein each behavior evaluation means records interesting function calls ~~some execution behaviors of~~that the code module makes as it is executed, , wherein the interesting function calls are specified by a user and comprise a subset of all function calls that the code module makes, wherein ~~a plurality of different execution behaviors of the code module~~only the interesting function calls, but not all function calls, that the code module makes during execution in the dynamic behavior evaluation module are recorded into a behavior signature corresponding to the code module;

a management means for obtaining the code module and determining the code module's type for the purpose of selecting a behavior evaluation means to execute the code module according to the code module's type;

a storage means for storing at least one known malware behavior signature of a known malware, wherein each of the at least one known malware behavior signature is comprised of only interesting function calls as specified by the user;

a behavior comparison means for comparing the behavior signature of the code module to the known malware behavior signatures in the storage means to determine whether the interesting function calls recorded in the behavior signature of the code module match the interesting function calls in any of the known malware behavior signatures; and ~~plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware; and~~

wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the ~~plurality of different execution behaviors~~interesting function calls recorded in the behavior signature of the code module match ~~at least one of a plurality of different subsets of execution behaviors recorded~~the interesting function calls in a behavior signature of the known malware~~, wherein the different subsets of execution behaviors are pre-specified for the known malware~~.

3. (Currently Amended) A method for determining whether a code module is malware according to the code module's exhibited behaviors, the method comprising:

receiving input from a user that specified interesting functions calls, wherein the interesting function calls are a subset of function calls that can be made by a code module;

receiving a code module to be evaluated to determine whether the code module includes malware;

selecting a dynamic behavior evaluation module according to the executable type of the code module as determined by a management module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording each interesting function call that the code module makes while being executed~~a plurality of different execution behaviors exhibited by the code module executing~~ in the dynamic behavior evaluation module to create a behavior signature for the code module ~~during execution of the code module~~;

comparing the recorded ~~plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module~~interesting function calls in the behavior signature for the code module to ~~a plurality of different execution behaviors~~interesting functions calls of a behavior signature of a known malware;

according to the results of the previous comparison, determining whether the code module is the known malware; and

reporting whether the code module is the known malware based at least in part on the degree that the ~~plurality of different execution behaviors~~interesting function calls recorded in the behavior signature of the code module match ~~at least one of a plurality of different subsets of execution behaviors~~the interesting function calls of the behavior signature of the known malware~~, wherein the different subsets of execution behaviors are pre-specified for the known malware~~.

4. (Currently Amended) A ~~computer-readable~~ storage medium storing computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors, the method comprising:

receiving input from a user that specified interesting functions calls, wherein the interesting function calls are a subset of function calls that can be made by a code module;

receiving a code module to be evaluated to determine whether the code module includes malware;

selecting a dynamic behavior evaluation module according to the executable type of the code module as determined by a management module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording each interesting function call that the code module makes while being executed~~a plurality of different execution behaviors exhibited by the code module executing~~ in the dynamic behavior evaluation module to create a behavior signature for the code module~~as the code module is executing~~;

comparing the recorded interesting function calls in the behavior signature for the code module ~~plurality of different recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module~~ to interesting function calls~~a plurality of different execution behaviors~~ of a behavior signature of a known malware;

according to the results of the previous comparison, determining whether the code module is the known malware; and

reporting whether the code module is the known malware based at least in part on the degree that the interesting function calls~~plurality of different execution behaviors~~ recorded in the behavior signature of the code module match the interesting function calls~~at least one of a plurality of different subsets of execution behaviors~~ of the behavior signature of the known malware~~, wherein the different subsets of execution behaviors are pre-specified for the known malware~~.

5-6. (Canceled)

7. (Currently Amended) The malware detection system of Claim ~~6~~1 or 2, wherein at least some of the ~~predefined set of execution behaviors to record corresponds to a set of~~interesting function calls are system calls.

8-12. (Canceled)

13. (Currently Amended) The method of Claim ~~12~~3, wherein at least some of the interesting function calls are~~the predefined set of execution behaviors to record corresponds to a set of~~ system calls.

14-15. (Canceled)

16. (Currently Amended) The ~~computer-readable~~ storage medium of Claim ~~14~~4, wherein at least some of the interesting function calls re ~~the predefined set of execution behaviors to record corresponds to a set of~~ system calls.

17. (Previously Presented) The malware detection system of Claim 1, wherein the malware detection system is further configured to report a positive identification of a known malware.

18. (Previously Presented) The malware detection system of Claim 2, wherein the malware detection system is further configured to report a positive identification of a known malware.

19-20. (Canceled)